MIP6 Working Group
INTERNET DRAFT
Informational
17 October 2005

Rajeev Koodli
Nokia Research Center

IP Address Location Privacy and Mobile IPv6: Problem Statement
draft-ietf-mip6-location-privacy-ps-00.txt

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This document is a submission of the IETF MIP6 WG. Comments should be directed to the MIP6 WG mailing list, mip6@ietf.org.

Abstract

In this document, we discuss Location Privacy as applicable to Mobile IPv6. We document the concerns arising from revealing Home Address to an on-looker and from disclosing Care of Address to a correspondent.

Contents

1. Introduction

The problems of location privacy, and privacy when using IP for communication have become important. IP privacy is broadly concerned with protecting user communication from unwittingly revealing information that could be used to analyze and gather sensitive user data. Examples include gathering data at certain vantage points, collecting information related to specific traffic, and monitoring (perhaps) certain populations of users for activity during specific times of the day, etc. In this document, we refer to this as the "profiling" problem.

Location privacy is concerned with the problem of revealing user roaming. A constant identifier with global scope can reveal that a user has roamed. The globally visible identifier could be a user identifier or a device identifier, and sometimes a binding between the two may also be available, e.g., through DNS. This problem is particularly applicable to Mobile IP where the Home Address on a visited network can reveal device roaming and, together with a user identifier (such as an NAI), can reveal user roaming. When roaming is revealed, it could lead to more targetted profiling. Even when the binding between user identifier and the Home Address is unavailable, freely available tools on the Internet can map the Home Address to the owner of the Home Prefix, which can reveal that a user from a particular ISP has roamed. So, the location privacy problem is a subset of the profiling problem in which revealing a globally visible identifier compromises a user's location privacy. In addition, a user may not wish to reveal roaming to correspondent(s). In Mobile IP, this translates to the use of Care of Address. In this document, the concerns arising from the use of a globally visible identifier, such as a Home Address, when roaming outside the home network are described. Similarly, the concerns from revealing a Care of Address to a correspondent are also outlined. The solutions to these problems are meant to be specified in a separate document.

This document is only concerned with IP Address Location Privacy in the presence of IP Mobility, as applied to Mobile IPv6. It does not address the overall profiling problem. Specifically, it does not concern itself with MAC addresses. Some other work may address the problem of profiling IP and MAC identifiers (see for instance [1]).

2. Problem Definition

2.1. Disclosing the Care of Address

When a Mobile IP MN roams from its home network to a visited network, use of Care of Address in communication with a correspondent reveals that the MN has roamed. The assumption here is that the correspondent somehow knows the Home Address of the MN. For instance, a correspondent may obtain it from DNS, which may contain the Home Address or the IP address of an agent to which the user identifier (such as a SIP URI) is mapped to.

2.2. Revealing the Home Address

When a Mobile IP MN roams from its home network to a visited network, use of Home Address in communication with a correspondent reveals to an on-looker that the MN has roamed. When a binding of Home Address to a user identifier (such as a SIP URI or NAI) is available, the

Home Address can be used to also determine that the user has roamed. This problem is independent of whether the MN uses Care of Address to communicate directly with the correspondent (i.e., uses route optimization), or the MN communicates via the Home Agent (i.e., uses reverse tunneling).

3. Problem Illustration

This section is intended to provide the overall scope under which the above problems are applicable.

Consider a Mobile Node at its home network. Whenever it is involved in IP communication, its correspondents can see an IP address valid on the home network. Elaborating further, the users involved in peer - peer communication are likely to see a user-friendly identifier such as a SIP URI, and the communication end-points in the IP stack will see IP addresses. Users uninterested in or unaware of IP communication details will not see any difference when the MN acquires a new IP address. Of course any user can ``tcpdump'' or ``ethereal'' a session, capture IP packets and map the MN's IP address to an approximate geo-location. When this mapping reveals a ``home location'' of the user, the correspondent can conclude that the user has not roamed. Assessing the physical location based on IP addresses is similar to assessing the geographical location based on the area-code of a telephone number. The granularity of the physical area corresponding to an IP address can vary depending on how sophisticated the available tools are, how often an ISP conducts its network re-numbering, etc.

Now consider that the MN roams to a new IP network, acquires a Care of Address and would like to communicate with its correspondents. It can either communicate directly or reverse tunnel its packets through the Home Agent. Using reverse tunneling does not reveal the new IP address of the MN, although performance may vary depending on the particular scenario. In some instances, the performance difference could be noticeable enough to serve as a hint to the correspondent. With those correspondents with which it can disclose its new IP address ``on the wire'', the MN has the option of using route-optimized communication. The transport protocol still sees the Home Address with route optimization. Unless the correspondent runs some packet capturing utility, the user cannot see which mode (reverse tunneling or route optimization) is being used, but knows that it is communicating with the same peer whose URI it knows. This is similar to conversing with a roaming cellphone user whose phone number, like the URI, remains unchanged.

Let us consider the roaming mobile node again. Regardless of whether

it uses route optimization or reverse tunneling, its Home Address is

revealed in data packets. When equipped with an ability to inspect packets ``on the wire'', an on-looker can determine that the MN has roamed and could possibly also determine that the user has roamed. This could compromise the location privacy even if the MN took steps to hide its roaming information from a correspondent.

The above description is valid regardless of whether a Home Address is static or is dynamically allocated. In either case, the mapping of IP address to geo-location will most likely yield results with the same level of granularity. With the freely available tools on the Internet, this granularity is the physical address of the ISP or the organization which registers ownership of a prefix chunk. Since an ISP or an organization is not, rightly, required to provide a blue-print of its subnets, the granularity remains fairly coarse for a mobile wireless network. However, sophisticated attackers might be able to conduct site mapping and obtain more fine-grained subnet information.

A compromise in location privacy could lead to more targetted profiling of user data. An eavesdropper may specifically track the traffic containing the Home Address, and monitor the movement of the Mobile Node with changing Care of Address. The profiling problem is not specific to Mobile IPv6, but could be triggered by a compromise in location privacy due to revealing the Home Address.
A correspondent may take advantage of the knowledge that a user has roamed when Care of Address is revealed, and modulate actions based on such a knowledge. Such an information could cause concern to a mobile user especially when the correspondent turns out be untrustworthy.

Finally, it is also worthwhile to note that both the Home Address and the Care of Address could be subject to profiling, just as any other user traffic. However, applying existing techniques to thwart profiling may have implications to Mobile IPv6 signaling performance. For instance, changing the Care of Address often would cause additional Return Routability and binding management signaling. And, changing the Home Address often has implications on IPSec security association management. These issues need to be addressed in the solutions.

4. Conclusion

In this document, we have formulated the IP Location Privacy problem in the presence of Mobile IPv6. The problem can be summarized as follows: disclosing Care of Address to a correspondent and revealing Home Address to an on-looker can compromise the location privacy of a Mobile Node, and hence that of a user. Solutions to this problem are

expected to specifically address the use of Mobile IPv6 addresses, and not other identifiers (such as MAC addresses).

5. IANA Considerations

There are no IANA considerations introduced by this draft.

6. Security Considerations

This document discusses location privacy because of IP mobility. Solutions to provide location privacy, especially any signaling over the Internet, must be secure in order to be effective. Individual solutions must describe the security implications.

7. Acknowledgment

James Kempf and Qiu Ying reviewed an earlier version and provided feedback.

References

[1] W. Haddad and et al. Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement (work in progress). Internet Draft, Internet Engineering Task Force, October 2004.

[2] J. Polk, J. Schnizlein, and M. Linsner. DHCP Option for Coordinate-based Location Configuration Information. Request for Comments 3825, Internet Engineering Task Force, July 2004.

8. Author's Address

Rajeev Koodli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043 USA
Phone: +1 650 625 2359
Fax: +1 650 625 2502
E-Mail: Rajeev.Koodli@nokia.com

A. Background

The location privacy topic is broad and often has different connotations. It also spans multiple layers in the OSI reference

model. Besides, there are attributes beyond an IP address alone that can reveal hints about location. For instance, even if a correspondent is communicating with the same end-point it is used to, the ``time of the day'' attribute can reveal a hint to the user. Some roaming cellphone users may have noticed that their SMS messages carry a timestamp of their ``home network'' timezone (for location privacy or otherwise) which can reveal that the user is in a different timezone when messages are sent during ``normal'' time of the day. Furthermore, tools exist on the Internet which can map an IP address to the physical address of an ISP or the organization which owns the prefix chunk. Taking this to another step, with in-built GPS receivers on IP hosts, applications can be devised to map geo-locations to IP network information. Even without GPS receivers, geo-location can also be obtained in environments where [Geopriv] is supported, for instance as a DHCP option [2].

In summary, a user's physical location can be determined or guessed with some certainty and with varying levels of granularity by different means even though IP addresses themselves do not inherently provide any geo-location information. It is perhaps useful to bear this broad scope in mind as the problem of IP address location privacy in the presence of IP Mobility is addressed.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.